Appendix F - Cyber-Security

Securing the State Of Michigan Information Technology Resources

Table of Contents

Executive Overview

The headlines say it all: "Internet attacks increase in number, severity." "Phishing attempts at record levels." "40 million credit card numbers hacked."

Professional criminals, not bored teenage hackers, are now the source of the most serious security threats. These threats require swift action and preventive measures. It is not just consumers who are at risk. On an average day, the state blocks 22,059 spam e-mails; 21,702 e-mail viruses; 4,239 Web defacements; and six remote computer take-over attempts.

Government today must balance the need for a citizen-centered e-government with the need to secure mission critical data and information. The challenge grows. With the increase in cyber crime, hacker attacks, threats from terrorists, and concerns about privacy, data confidentiality, integrity, and availability as well as strong and flexible authentication and authorization methods are critical to securing information, increasing efficiency, and reducing cost.

With more demand from remote workers, citizens who expect 24/7 access to information and services and increased federal requirements for protecting data both in storage and in transmission come the need for more robust security management systems. The State of Michigan has won awards in the area of cyber-security with its mature architecture model.

To date, the State of Michigan has instituted or initiated several projects to reduce vulnerabilities, including:

- Digital video manager equipment to provide physical security at three critical IT data centers
- Tools to monitor firewalls, intrusion detection systems, networking devices and other applications, searching for threat patterns
- Scanning systems that identify threats on the wired network and detect rogue or unauthorized wireless access points that may have been installed
- Authentication and access control projects that filter e-mail and help manage spam and viruses coming into the network
- Zone 3 fire walls have been implemented at each hosting center.

Additionally, the state seeks to educate the public on ways they can protect themselves from identity theft, computer viruses, fraud and other risks. A new Web portal - www.michigan.gov/cybersecurity - was launched with tips on how citizens can protect confidential information, physical security and other security best practices.

Importance to Citizens, Businesses and Government

With the increasing demand for citizen-centered e-government and online services, one of government's most important responsibilities is securing sensitive information. These requirements, along with the ability to share information inter- and intra-agency, have presented a host of security challenges. With the increase in cyber crime, hacker attacks, threats from terrorists, and concerns about privacy, data confidentiality, integrity, and availability as well as strong and flexible authentication and authorization methods are critical to securing information, increasing efficiency, and reducing cost.

Professional criminals, not bored teenage hackers, are now the source of the most serious security threats. New regulations in the areas of privacy and governance are bringing the focus of IT security threats to center stage in order to better understand how best to manage and protect citizen and government information. Federal and state regulations, such as Federal Information Processing Standard (FIPS) 140-2 to ensure integrity and privacy of messages, Michigan's Social Security Number Privacy Act, Driver's Privacy Protection Act of 1994, Fair Credit Reporting Act of 1970, Gramm-Leach-Bliley Financial Services Modernization Act of 1999, the Health Insurance Portability and Accountability Act (HIPAA) of 1996, and the Sarbanes-Oxley Act of 2002, require that data is protected and remains confidential in storage and in transmission.

In order to meet these requirements and provide the necessary services to citizens, security management systems are crucial. One of the most widely adopted information security management frameworks, ISO/IEC 17799:2005 provides a strong and expanded framework for information security management. It pays specific attention to risk assessment, provides incident management guidance details, integrates other ISO standards, addresses security in business partner relationships and provides guidance on technical vulnerability management.

Specific focus on IT security today is a result of threats from the Internet. For example, in 2004 53 percent of all reported fraud complaints to the Federal Trade Commission (FTC) were Internet-related (e.g. spam, phishing, spyware, and other malware threats). In addition, nearly 5 percent of Americans have been victims of identity theft within the past five years and financial losses due to identity theft are estimated at $48 billion per year. It is reported that government systems (e.g. tax systems, driver's license applications, etc.) are the fastest growing areas where identity theft occurs. This emphasizes that the State of Michigan must do everything possible to mitigate IT risks and ensure citizens' private information is protected from exploitation, misuse, or disclosure.

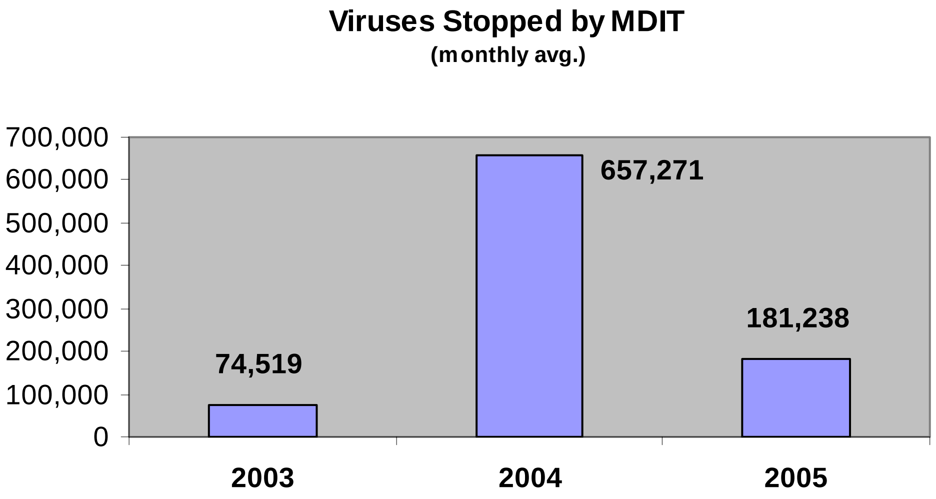
Emergency Management and Preparedness

The Department of Information Technology (MDIT) plays an active role in preparing for, training for, and responding to emergency events. If the governor declares an emergency, Michigan's State Emergency Operations Center (SEOC) will activate. MDIT's Emergency Management Coordinator (EMC) will be notified and immediately proceed to the SEOC to coordinate MDIT's response to the event. The EMC will notify MDIT's executive management and, if appropriate, activate MDIT's Emergency Coordination Center to carry out resource coordination and response efforts within MDIT. Because technology plays a vital role in the business of each agency and state government as a whole, MDIT's efforts to respond to an emergency can be significant. The emergency event does not need to be strictly cyber, as MDIT supported the Katrina and Rita relief efforts when the SEOC was activated for the hurricane disasters. MDIT has sponsored and participated in many emergency preparedness exercises that play out scenarios to test response plans' effectiveness. In addition, many key MDIT staff, from executives to responders, will be trained in 2006 in the National Incident Management System and the National Response Plan.

In February 2006 MDIT will participate in the nation-wide Cyber Storm exercise sponsored by the U.S. Department of Homeland Security. The purpose of this exercise is to raise awareness of the economic and national security impacts associated with a significant cyber incident. Participants will include fifteen or more federal agencies, including the FBI, CIA, NSA, and Secret Service; three states, including Michigan; and four other countries.

Current Security Accomplishments

The State of Michigan has experienced ongoing cyber attacks against its IT resources. Based on 2004 averaged statistics taken from gateway system logs, the state saw 21,702 daily e-mail virus attack attempts; 35,383 daily scanning attempts for unauthorized access; 4,239 daily Web defacement attempts; and six daily computer remote-control takeover attempts. The state is effectively securing IT assets and resources as demonstrated by the fact that these attempts were preempted. However, cyber criminals have become very adept at circumventing traditional defenses, and it is imperative that the state is prepared to remain one step ahead of the attackers.



Through the fiscal year 2004 State Homeland Security Grant Program (SHSGP), the State of Michigan was awarded $14.9 million for critical infrastructure protection projects. Of the state's award, the MDIT was awarded $4.1 million to reduce vulnerabilities and mitigate risks to critical cyber and telecommunication infrastructure.

Several projects were initiated to accomplish Michigan's homeland security protection goals during 2004:

- Ensuring IT systems are up and running consistently is a critical piece of continuity of government requirements. The state purchased two large fixed generators for the state's data centers to support critical State of Michigan applications in case of power failures.

- A digital video manager equipment project provides physical security at the three critical IT data centers. This facilitates better access control and surveillance of critical IT infrastructure to protect against physical attacks. This system also provides auditing and deterrence for attackers.

Several projects addressed the concerns of cyber intrusion detection:

- The event correlation solution accumulates data from various security systems such as firewalls, network-based intrusion detection systems, host-based intrusion detection systems, networking devices, and other application sources and searches for significant threat patterns within limited timeframes.

- The network intrusion detection project determines the location and nature of a cyber attack originating from internal resources against resources in consolidated data centers.

- Network traffic tools allow the capture and analysis of suspicious and potentially destructive or intrusive network traffic at strategic network locations to avoid or mitigate cyber attacks (such as denial-of-service) against critical state IT infrastructure.

- Cyber incident investigation and response technologies include a vulnerability scanning project that identifies known and unknown vulnerabilities, suggests fixes, and reports possible security holes within the state's networks. Vulnerability scanning identifies threats on the wired network and also detects rogue or unauthorized wireless access points that may have been installed.

- A project for the forensic recovery of evidence was launched in order to respond and recover from a cyber-related incident against the State of Michigan's critical infrastructure. Forensic examination is accomplished through special hardware devices and software that prevent compromising or contaminating evidence for the use of investigation or potential criminal prosecution. A second part of this project is the Rimage system that is used to distribute to law enforcement, via DVD, information (e.g., video surveillance) and evidence of the cyber-related incident.

- Network scanning and penetration studies and assessment were accomplished that identified potential entryways into vital or sensitive data within the state's network. Potential vulnerabilities were patched and mitigated, ensuring protection of state assets.

- The Forensic Analysis of Risks in Enterprise Systems (FARES) solution built a model of possible outcomes of mitigation strategies that will be used for on-going impact analysis. FARES delivers a model of the enterprise for risk mitigation strategies.

Two important authentication and access control projects have demonstrated significant benefits in protecting government resources and providing cost savings:

- E-mail and spam and filtering software are integrated on servers at the state's gateway. This solution filters spam and serves as the state's anti-virus solution for incoming and outgoing e-mail. After Internet e-mails are filtered through the anti-virus gateway, the State of Michigan is left with approximately 4.8 million e-mails per month. About 54 percent of these are spam. The average monthly spam e-mails blocked at the Internet gateway total 2.6 million. The anti-spam implementation at the gateway shows a return on investment in number of blocked spam e-mails that would have taken time away from business-related efforts. The annual anti-spam savings total as much as $15.7 million.

- SurfControl Internet Access Control and Filtering Systems prevent system users from accessing Web sites that are deemed risks to the state's network and systems. They are used to protect against the possible disclosure of confidential information, help to ensure worker productivity by preventing access to sites that are not business related, and protect the networks from valuable bandwidth diversion and system infections (e.g., viruses, worms, Trojan programs, spyware, fraud and scam sites, etc.). SurfControl metrics show that approximately 80,000 blocked connection attempts to spyware Web sites occur every month. SurfControl's spyware block shows an annual cost savings of approximately $3.3 million.

The IT Security Awareness Web Portal (**www.michigan.gov/cybersecurity**) provides IT security information for computer users throughout Michigan. This Web site reaches out to all citizens of Michigan, state employees, and home computer users everywhere with the purpose of providing a better understanding of security issues such as computer virus threats, protection of confidential and sensitive information, Internet and e-mail usage, physical security, wireless risks, recommendations for avoiding fraud and identity theft, and best practice.

The Office of Enterprise Security (OES) is accountable to the MDIT director for identifying, managing, and mitigating IT security risks and vulnerabilities within State of Michigan government computing, communication, and technology resources. OES is also charged with the oversight of disaster recovery planning, IT security risk management, IT security awareness and training, working with state agencies to assist with their security issues, and enforcement oversight of state security policies and procedures intended to maintain appropriate levels of enterprise-wide security.

IT Security Goals

Automated Patch Management and Policy Compliance

The state requires an automated means of determining if mobile and wireless computers from outside of the state's network connecting into the state's network are compliant with State of Michigan security policies. Ensuring all remote computer systems have appropriate anti-virus protection with current virus signatures, appropriate security patches for the operating systems used in the enterprise, firewalls for mobile devices, secured accounts, and systems that are configured to approved security policy is necessary to reduce the vulnerabilities to critical infrastructure. The purpose is to ensure security policy compliance through quarantine and remediation of the mobile and wireless devices not meeting the set security policy whenever these devices connect to the network.

In addition, the automated patch management and policy compliance project must include a vulnerability management process that ensures all servers and network devices are compliant with security policy. Automated remediation of noncompliant devices that are denied access or placed in quarantine will minimize both downtime and connect time for those devices. Because manual remediation processes are ineffective in a reasonable timeframe, utilize staff resources that are short in supply, and are difficult to implement in an enterprise setting with multiple platforms, it is imperative to have an automated process that maps to a consistent set of security policies.

Measurements of number of devices remediated, DIT staff time saved from repairs, number of security patches applied, and device downtime avoided will all indicate return on investment metrics as well as protections applied.

Identity and Access Management

In the efforts to combat identity theft and adhere to privacy regulations, an identity and access management solution is necessary to secure Web-based systems, data sharing, and mobile computing technologies as these are implemented in the state. Many think of single sign-on as the flagship of identity management. However, it is much more than simple password management or reduced sign-on. Identity management is an integration architecture that provides centralized control, authentication, administration, authorization, audit, and compliance management for all events related to resource access (e.g. password management, provisioning, mobile access, and Web interface self service applications). Providing IT addresses keys compliance concerns around documentation, enforcement, and auditing of security controls, as well as managing user accounts and profiles that link users to roles and business rules across the IT environment. The primary value of provisioning focuses on policy enforcement and audit ability around role-based access controls and centralized process management. The concept of identity is not restricted to people. Devices, applications, and physical assets comprise additional identities that need to be managed in an increasingly networked and interconnected environment.

Currently, there is not a standardized implementation of identity and access management in the State of Michigan. An access control model for employee, authorized agent, and public identity and security management must be developed. A determination of data sources, services and applications, devices, and service directories must be assessed. Meta-directories are software products that synchronize and aggregate identity data stored in multiple repositories. This can provide an effective way to reduce user administration by synchronizing the identity data across the data identity stores.

The identity and access management solution must be able to identify and authenticate each requestor (user, device, application, etc.), authorize each request for the specific resource based on the requestor's identity, analyze sessions to ensure actions are not malicious, and audit the activity on per requestor and per resource bases for compliance and audit. It is recommended to prioritize projects based on demand and complexity and then roll out the processes incrementally to systems that would benefit most from the identity management processes.

Measurements of identity and access management benefits can be derived from reductions in user administration, speed and agility of customer resource access, identity store synchronization, audit and accountability of actions, and privacy protections provided to confidential data.

OTAR Encryption

About 2,200 Michigan Public Safety Communications System (MPSCS) law enforcement and emergency responder users have encrypted voice communication and the need will continue to grow. The process to change keys is logistically very difficult as every radio has to be physically handled. Therefore there is a need to implement an automated, over-the-air-re-keying (OTAR) system.

An OTAR encryption key management system provides automated capabilities to manage the encryption keys to protect voice and data transmission from unauthorized listening. OTAR gives a system operator the capability of regularly, remotely and securely changing keys over the air.

Measurements for OTAR benefits can be calculated through the savings made by replacing manual processes. As an example, the radio technician costs for changing the keys on all 2,200 radios today would equal about $16,000 (one Network Control Center technician could re-key 40 radios in a day. One technician would use 55 days to re-key the 2,200 radios. Salary and wages for a day equals about $290.) This cost does not include the time users lose dropping off and picking up the radios, opportunities lost when the radios are in the shop, or the cost of delaying other tasks as the NCC assigns resources to perform the re-keying. Approximately two hours per radio would be lost at an additional cost of about $160,000 (4,400 hours @ $36/hr).

Both the costs and logistical problems of regular re-keying drive the need for MPSCS to implement an automated version of this process.

Summary

In conclusion, the current level of cyber and communication protection in the State of Michigan has significantly improved as a result of Michigan's homeland security initiatives. However, gaps remain that require additional attention to ensure the state is prepared for cyber attacks against critical IT infrastructure. The key driver for the automated patch management and policy compliance project, identity and access management, and OTAR encryption key management is regulatory compliance. However, the three targeted goals will also facilitate cost containment and more effective business operations. Through the implementation of the targeted IT security goals, the level of cyber protection in the State of Michigan will improve appreciably.